UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Kelly Richards, DOB: XX/XX/1980, Social Security Account Number XXX-XX-8394	)	Case No. **1:23-MJ-00398**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-3

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2422(b)	Coercion and Enticement
18 U.S.C. §§ 1591 & 1594	Sex Trafficking of Children & Attempt/Conspiracy
18 U.S.C. § 2251	Sexual Exploitation of Children

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Nathan Holbrook
Applicant's signature

Nathan Holbrook, Special Agent FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by FaceTime video conference *(specify reliable electronic means)*.

Date: **May 12, 2023**

Stephanie K. Bowman
Judge's signature

City and state: Cincinnati, Ohio

Stephanie K. Bowman, United States Magistrate Judge
Printed name and title

ATTACHMENT A-3

The premises to be searched is the person of Kelly Richards, further described as a black male born on October XX, 1980, with Social Security Account Number of XXX-XX-8394. Richards is approximately 5 feet and 7 inches tall, with black hair and brown eyes. Richards has a scorpion tattoo on the left side of his face. The premises to be searched also includes any clothing Richards is wearing at the time of the search, as well as any bags or containers on Richard's person or within his reach at the time of the search. Attached is a BMV photo of Richards.

ATTACHMENT B

Particular Things to be Seized

1. Computer(s), cellphone(s), tablet(s), computer hardware (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives, diskettes, and other memory storage devices), computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography, child erotica, or to prostitution or sex trafficking of a minor.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography, or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct, or to sex trafficking or prostitution.

4. In any format or medium, all child pornography or child erotica.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer, or by other means for the purpose of distributing or receiving child pornography, visual depictions, or the prostitution or sex trafficking of a minor.

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by computer, any child pornography, visual depictions, or the prostitution or sex trafficking of a minor.

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography, visual depictions, or the prostitution or sex trafficking of a minor

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography, or the existence of sites on the Internet that contain child pornography or that cater to whose with an interest in child pornography or the prostitution or sex trafficking of a minor.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members or the prostitution or sex trafficking of a minor.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.

13. Any and all cameras, film, videotapes or other photographic equipment.

14. Any and all visual depictions of minors in order to compare the images to known and identified minor victims of sexual exploitation or sex trafficking.

15. Any and all address books, mailing lists, supplier lists, mailing address labels, and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography or any visual depictions, or the prostitution or sex trafficking of a minor.

16. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages,

and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

17. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.
18. Any records, bills, or other documents associated with internet service providers and telephone services.

19. Any records or communications in which sexually explicit material is being sent or received and any records or communications relating to prostitution or sex trafficking of a minor.

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Nathan Holbrook, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation and have been since February 13, 2011. In July 2011, I was assigned to the Indianapolis Division, Merrillville Resident Agency to work white collar crimes and public corruption investigations. In joining the FBI as a Special Agent, I initially spent five months at the FBI training academy in Quantico, Virginia, where I studied numerous investigative techniques, including those involved in white collar/public corruption investigations.

2. I was a member of the Northwest Indiana Public Corruption Task Force from August 2011 until December 2017. This task force focused on public corruption investigations throughout Northwest Indiana and was comprised of several federal law enforcement agencies, including the FBI and the Internal Revenue Service (IRS). As part of my duties while a member of this task force, I was involved in numerous public corruption investigations including investigations of elected public officials, non-elected government employees, and corrupt law enforcement officers. In the course of these investigations, and through my involvement in other investigations with other experienced white collar/public corruption investigators, I have participated in white collar and/or public corruption investigations involving the use of Title III communication intercepts, confidential surreptitious undercover recordings, electronic tracking devices, pen registers and trap and trace devices, and various types of search warrants for GPS location information, government offices, and government computer systems.

3. In January of 2018, I was transferred to the Cincinnati Division of the FBI and assigned to a white collar/public corruption unit, specifically to investigate public corruption in Southern Ohio to include bribery, extortion, and theft of funds from programs receiving government money. Since my assignment to the Cincinnati Division, I have conducted or participated in public corruption investigations utilizing advanced techniques to include the use of: Undercover Agents; confidential human sources; consensual undercover recordings; Title III communication intercepts; physical surveillance; pen registers and trap and trace devices; and the analysis of financial records.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence of violations of Title 18 U.S.C. §§ 1591 & 1594 (Sex Trafficking of Children to include attempting and conspiring), Title 18 U.S.C. § 2422(b) (Coercion & Enticement for Illegal Sexual Activity to include attempting) and Title 18 U.S.C. § 2251 (Sexual Exploitation of Children) the "subject offenses" have been committed by Kelly Richards and other persons unknown. There is probable cause to search the residence, vehicle, and person described in Attachments A-1 through A-3 for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachments B.

6. This Affidavit is submitted in support of Applications for search warrants for the following:

a. The residence located at 1828 Sunset Avenue, Apartment 26, Cincinnati, Ohio, which is an apartment located in a three-story apartment building more fully described in Attachment A-1
b. A silver 2009 Infiniti SUV bearing Ohio license plate PLJ1198, more fully described in Attachment A-2
c. The person known as Kelly Richards, DOB: XX/XX/1980, Social Security Account Number XXX-XX-8394, including any bags or objects closely associated with his person, and more fully described in Attachment A-3

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachments to this Affidavit:

a. **"Child Pornography"** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

b. **"Visual depictions"** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).

c. **"Minor"** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).

d. **"Sexually explicit conduct"** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of

the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2))

e. **"Internet Service Providers"** or **"ISPs**" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone-based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a username or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

f. A network **"server"**, also referred to as a **"host"**, is a computer system that has been designated to run a specific server application or applications and provide requested services to a "client" computer. A server can be configured to provide a wide variety of services over a network, including functioning as a web server,

mail server, database server, backup server, print server, FTP (File Transfer Protocol) server, DNS (Domain Name System) server, to name just a few.

g. **"Domain Name"** refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top level domains are typically ".com" for commercial organizations, ".gov" for the governmental organizations, ".org" for organizations, and, ".edu" for educational organizations. Second level names will further identify the organization, for example "usdoj.gov" further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government. The Domain Name System, also referred to DNS, is a system of servers connected to each other using a common system of databases that resolve a particular domain name, such as "www.usdoj.gov," to its currently assigned IP address (i.e., 149.101.1.32), to enable the follow of traffic across the Internet.

h. An **"Internet Protocol address"**, also referred to as an **"IP address"**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a

unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as "octets," ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is connected to the Internet (or other network).

i. **"Log Files"** are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

j. **"Hyperlink"** (often referred to simply as a **"link"**) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. "resource") to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.

k. **"Website"** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

l. **"URL"** or "Uniform Resource Locator" or "Universal Resource Locator" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

m. The terms **"records"**, **"documents"**, and **"materials"**, as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic

notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

CHARACTERISTICS COMMON TO INDIVIDUALS WITH INTENT TO COLLECT, RECEIVE OR DISTRIBUTE CHILD PORNOGRAPHY

8. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals with intent to view and/or possess, collect, receive, or distribute images of child pornography:

a. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Furth Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of

children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain photos, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals with intent to view and/or possess, collect, receive, or distribute pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

e. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone

numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who would have knowledge about how to access online forums, such as bulletin boards, newsgroups, Internet relay chat or chat rooms are considered more advanced users and therefore more experienced in acquiring and storing a collection of child pornography images.

g. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

9. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

10. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 64 gigabytes of data, which provides enough space to store thousands of high-

resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer. Additionally, almost all cell phones today can record high-resolution photographs and videos.

11. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

12. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera or a cell phone, upload that photo to a

computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.

13. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

14. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

15. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

BACKGROUND REGARDING SEIZURE OF COMPUTERS

16. As stated, the investigation has determined that one or more computers (to include cellphones) have been used as an instrumentality in the course of, and in furtherance of, the offenses described above. Moreover, it is reasonable to believe that records and evidence are being stored in electronic form. This includes computer hard-drives, disks, CDs, modern cellphones and other similar electronic storage devices.

17. As indicated above, computer hardware is used to save copies of files and communications, while printers are used to make paper copies of same. Programs loaded on the drives are the means by which the computer can send, print and save those files and communications. Finally, password and security devices are often used to restrict access to or hide computer software, documentation or data. Each of these parts of the computer is thus integrated into the entire operation of a computer. In order to best evaluate the evidence, the computers—and all of the related computer equipment described above—should be available to a computer investigator/analyst.

Forensic Imaging

18. An important step that is ordinarily part of an expert's forensic examination of a computer involves attempting to create an electronic "image" of those parts of the computer that are likely to store the evidence, fruits, instrumentalities, or contraband relating to the applicable offense. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files.

19. Special software, methodology and equipment are used to obtain forensic images. Among other things, forensic images normally are "hashed," that is, subjected to a mathematical algorithm to the granularity of 1038 power, which is an incredibly large

number that is much more accurate than the best DNA testing available today. The resulting number, known as a "hash value" confirms that the forensic image is an exact copy of the original and also serves to protect the integrity of the image in perpetuity. Any change, no matter how small, to the forensic image will affect the hash value so that the image can no longer be verified as a true copy.

Forensic Analysis

20. After obtaining a forensic image, the data will be analyzed. Analysis of the data following the creation of the forensic image is a highly technical process that requires specific expertise, equipment and software. There are literally thousands of different hardware items and software programs that can be commercially purchased, installed and custom-configured on a user's computer system. Computers are easily customized by their users. Even apparently identical computers in an office environment can be significantly different with respect to configuration, including permissions and access rights, passwords, data storage and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

21. Analyzing the contents of a computer, in addition to requiring special technical skills, equipment and software also can be very tedious. It can take days to properly search a single hard drive for specific data. Searching by keywords, for example, often yields many thousands of "hits," each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. The computer may have stored information about the data at issue: who created it; when it was created; when it was last accessed; when it was last

modified; when was it last printed; and when it was deleted. Operation of the computer by non-forensic technicians effectively destroys this and other trace evidence.

22. Moreover, certain file formats do not lend themselves to keyword searches. Keywords search for information in text format. Many common electronic mail, database and spreadsheet applications do not store data as searchable text. The contents of Adobe ".pdf" files are not searchable via keyword searches. The data is saved in a proprietary non-text format. Microsoft Outlook data is an example of a commonly used email program that stores data in a non-textual, proprietary manner–ordinary keyword searches will not reach this data. Documents printed by the computer, even if the document never was saved to the hard drive, are recoverable by forensic examiners, yet they are not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. Similarly, faxes sent to the computer are stored as graphic images and not as text.

23. Analyzing data on-site has become increasingly impossible as the volume of data stored on a typical computer system has become mind-boggling. For example, a single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now capable of storing more than 100 gigabytes of data and are commonplace in new desktop computers. And, this data may be stored in a variety of formats or encrypted. The sheer volume of data also has extended the time that it takes to analyze data in a laboratory. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. Even perusing file structures can be laborious if the user is well-organized. Producing only a directory listing of a home

computer can result in thousands of pages of printed material most of which likely will be of limited probative value.

24. Based on the foregoing, searching any computer or forensic image for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques, and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained. Evidence in graphic file format must be laboriously reviewed by examiners. Criminals can mislabel and hide files and directories, use codes to avoid using keywords, encrypt files, deliberately misspell certain words, delete files, and take other steps to defeat law enforcement.

Persistence of Digital Evidence

25. Computers store data, both on removable media (for example, CDs and floppy diskettes) and internal media, in ways that are not completely known or controlled by most users. Once stored, data is usually not destroyed until it is overwritten. For example, data that is "deleted" by a user is usually not actually deleted until it is overwritten by machine processes (rather than user decision) that decide where to store data and when overwriting will occur. Therefore, files and fragments of files and other data may easily last months, if not years, if the storage media is retained.

26. Typically, computer forensics focuses on at least three categories of data. These are: 1) **active data** – such as current files on the computer, still visible in file directories and available to the software applications loaded on the computer; 2) **latent data** – such as deleted files and other data that resides on a computer's hard drive and other electronic media in areas available for data storage, but which are usually inaccessible without the use of

specialized forensic tools and techniques; and 3) archival data – such as data which has been transferred or backed up to other media such as CDs, floppy disks, tapes, and ZIP disks.

27. **Active data** includes not only files created by and with the user's knowledge, but also may include items such as Internet history log files, system registry files (listing all the systems and software applications installed on a computer, including the dates of installation, use, and deletion), and date/time file stamps automatically created that identify when files were created, modified, and last accessed.

28. **Latent data** includes data retained and stored on computer media in "unallocated" and "slack" space. Unallocated space refers to space on a hard drive that is available for the storage of new data. Slack space refers to any leftover space that remains when an active file is stored in particular location on the hard drive that is akin to an empty shelf in a closet containing other full shelves. Deleted files and other latent data that has not been overwritten by new data or files often may be accessed by a qualified forensic examiner from the unallocated and slack space on a computer user's hard drive months and years after such data was created by the user or the computer's operating system.

29. I know, based upon my training and experience, that a qualified forensic examiner may use knowledge of the mechanisms used to store electronic data to unlock and to uncover the activities of a computer's user years after the fact by examination of active, latent, and archival data. Through the use of proper computer forensic techniques such data and evidence of criminal offenses may be recovered, notwithstanding the passage of time since a crime occurred.

Conclusion Regarding Forensic Analysis Procedures

30. In light of these difficulties, I request permission for investigators to remove to a forensically-secure location the computers and computer-related equipment as instrumentality(ies) of the crimes, and to use whatever data analysis techniques reasonably appear necessary to locate and retrieve digital evidence within the scope of this warrant. Such action will greatly diminish the intrusion of law enforcement into the premises and will ensure that evidence can be searched for without the risk of losing, destroying or missing the information/data for which there has been authorization to search.

31. Therefore, it is respectfully requested that the warrant sought by this application authorize the search and seizure for all "computer hardware," "computer software" and documents, which are more fully set-out and explained above, and further authorize a full physical and forensic examination of the seized items at a secure location.

PROBABLE CAUSE

32. In March of 2023, Investigators were told by the Anti-Human Trafficking Coordinator with the Hamilton County Juvenile Court, that two minor females had been screened as possible sex trafficking victims.

33. On March 16, 2023, Minor Victim 1 (hereafter referred to as MV1), date of birth XX/XX/2008, was interviewed by a forensic interviewer at Cincinnati Children's Hospital. MV1 was at a group home named Hope Haven for girls located in Dayton, Ohio. While at Hope Haven, MV1 met Minor Victim 2 (hereafter referred to as MV2), date of birth XX/XX/2008. On approximately February 28, 2023, MV1 and MV2 ran away from Hope Haven. MV2 told MV1 they were just going around the block to smoke marijuana with a friend of MV1's, referred to as "Scorpio." MV1 and MV2 ran away from Hope Haven for about two blocks and waited approximately 15 minutes, but Scorpio did not arrive. They walked back to Hope Haven and MV2 knocked on her roommate's window for the purpose

of having the roommate log onto Facebook to contact Scorpio. At approximately the same time, Scorpio drove by, eventually stopping and picking up MV1 and MV2. MV1 described Scorpio's vehicle as a tan or silver color sport utility vehicle. MV1 described Scorpio as a dark-skinned male with very short hair. He had a scorpion tattoo on his face with a piercing at the point of the scorpion tail. Scorpio drove MV1 and MV2 to an apartment complex in Cincinnati located at 1828 Sunset Avenue.

34. On March 22, 2023, investigators conducted surveillance in the area of 1828 Sunset Avenue, Cincinnati, Ohio and observed a large Infiniti SUV that fit the description of the vehicle Scorpio used to pick up MV1 and MV2. The vehicle had an Ohio license plate PLJ1198. The license plate number was searched in a police database and found to be associated with a 2009 Infiniti SUV and registered to Scorpio's One Stop Shop, LLC, 9125 Winston Road, Apartment 13, Cincinnati, Ohio. A search of the Ohio Secretary of State Business Search website showed Scorpio's One Stop Shop, LLC is registered to Kelly Richards (hereafter referred to as "Richards"), PO Box 428786, Blue Ash, Ohio, 45242. Investigators obtained a Bureau of Motor Vehicle's photograph of Richards. Richards fit the description provided by MV1 to include the scorpion tattoo on his face.

35. Once inside Richards' apartment, MV1 was offered a plate that contained cocaine and she did a line. MV1 said she was scared because she did not know where she was or what was going to happen to her. Richards received a phone call from an individual MV1 referred to as "Bear." Shortly after, Bear comes to Richards' apartment. MV1 observed Richards sell cocaine to Bear. Richards also retrieved two guns from his bedroom and gave them to Bear.

36. Richards, MV1, and MV2 did additional lines of cocaine and then went into Richards' bedroom. MV1 sat on the side of Richards' bed while MV2 and Richards had sex. After sex with MV2, MV1 said Richards made MV2 "touch me and eat me and stuff like that and it made me very uncomfortable." MV1 said Richards told MV2 to "sixty-nine, eat me out and like to kiss me and stuff, to finger me." MV2 was touching MV1's vagina with her tongue and placing MV2's fingers in MV1's vagina. Richards eventually pushed MV2 off and engaged MV1 in vaginal sex. Richards did not ask MV1 for consent to have sex with her. Richards also made MV1 give him oral sex that same night.

37. The following day, on or about March 1, 2023, they ordered pizza from LaRosa's. Investigators obtained an order receipt from LaRosa's dated March 1, 2023. The receipt listed the customer's name as Scorpio with a telephone number of 513-668-6630 and address of 1828 Sunset Avenue, Cincinnati, Ohio.[1] The receipt had an order time of 9:14 PM. Toll records indicated that telephone number 513-668-6630 called LaRosa's located at 4008 Glenway, Avenue, Cincinnati, Ohio at 9:10 PM on March 1, 2023. The AT&T records also indicated the phone associated with telephone number 513-668-6630 was an Apple iPhone 11 Pro Max with IMEI number of 3538901085912822 and IMSI number of 310410262344029.

38. On the same night, Richards told MV1 that if his friend "Lorenzo" wanted to have sex with her it would cost him $100. MV1 asked Richards what if she did not want to have sex with Lorenzo. Richards told MV1 to just do it because they needed the money. MV1 described Lorenzo as an older male, approximately 57 years old. Lorenzo came to Richards' apartment and asked MV1 to come to his (Lorenzo) apartment. MV1 went with Lorenzo

[1] Subscriber information and toll records were obtained from AT&T by administrative subpoena for telephone number 513-668-6630.

because she was scared not to do what Richards told her to do. Lorenzo began taking off MV1's clothes, but she stopped him and said he would have to pay first before having sex with MV1. Lorenzo agreed to give MV1 $30 in exchange for sex. After the sexual encounter with Lorenzo, MV1 returned to Richards' apartment. Richards was mad at MV1 because she took too long and only made $30. Richards took the $30 and screamed at MV1. MV1 said, "Scorpio (Richards) was making me, like, have sex with these people and get paid, and give him the money."

39. On or about March 2, 2023, Richards obtained assistance from an unknown female who went by the name "Red." Richards commented about how MV1 could make real money and asked Red if she could help out. MV1 said Red was a prostitute and utilized an online application called "link finder or crawler" where girls advertised themselves for sex in exchange for money. Richards wanted to post an ad online advertising MV1 and MV2 for prostitution. Richards used an account that was associated with Red's boyfriend's daughter. Richards used the account to post an advertisement, depicting photos of MV1 and MV2. Red provided the account information to Richards. MV1 remembered the account password was "starburst." MV1 said Richards was the one who controlled everything.

40. Richards' iPhone was used to take pictures of MV1 in the shower, which showed MV1 undressed from her upper thighs to her neck, depicting MV1's breasts and vagina. Additional photos were taken of MV1 laying down on Richards' bed showing her back. MV1 believed the covers on Richards' bed were striped. None of the photos contained MV1's face. The photos were used in the ad online advertising for sex. Photographs of MV2, which included her face, breasts, and backside were placed in an advertisement. MV1 was referred to as "Essence" in the ad. Richards received a lot of responses from the

advertisements. MV1 said Richards had two phones, a red iPhone 7 or 8, and a red iPhone 11.2 MV1 said the account for the ad was on the iPhone 7 or 8. The number on the ad would go to Richards' iPhone 11. MV1 believed Richards' iPhone service provider was AT&T. Richards took photos of MV2 using his iPhone 11 and uploaded them to the ad. The photos of MV2 included her face and breasts.

41. An unknown male (UM1) responded to the advertisement for MV1 saying he would pay $125 for oral sex. Richards and MV2 drove MV1 to meet UM1 at his residence. MV1 said she was scared. She didn't know anything other than "there's a dude who wanted head and I had to do it." MV1 gave UM1 oral sex in exchange for $120. MV1 told investigators that MV2 had four dates consecutively the same day at both hotels and homes, earning $365. Richards referred to the dates as "licks." MV1 said the dates were set up by individuals contacting a telephone number on the ad which would go to Scorpio's phone.

42. On or about March 3, 2023, Lorenzo came over to Richards' apartment. Lorenzo wanted MV1 to come back over to his apartment. Richards told MV1 to go to Lorenzo's apartment and try to make some money. At Lorenzo's apartment, Lorenzo told MV1 to take off her clothes, but MV1 told Lorenzo he had to pay her first. MV1 and Lorenzo talked for approximately 45 minutes without engaging in sex. When MV1 returned to Richards' apartment without money, Richards screamed at her. Richards told MV1 to sit next to him which she did. Richards asked her why he shouldn't smack the shit out of her. MV1 responded that she did not know and stood up to walk away, at which point Richards struck MV1 on the back of the neck.

[2] In a follow-up interview with investigators, MV1 said the older iPhone might have been an iPhone 8 or 9.

43. MV2 was interviewed by investigators on April 6, 2023. MV2 had known Richards for approximately one year. MV2 contacted Richards to collect her and MV1 from Hope Haven via Facebook Messenger. Richards' Facebook account was Scor Pio.3 MV2 said Richards picked them (MV1 and MV2) up from Hope Haven and drove them to his apartment. MV2 said Richards' apartment was located on Sunset Avenue in the Westwood area of Cincinnati, and specifically described the location of his apartment at the bottom of the stairs next to a laundry room. MV2 showed investigators a map of the location of Richards' apartment on her phone. The location was consistent with 1828 Sunset Avenue. While at the apartment, Richards had MV1 take photos of MV2 undressed. Scorpio placed the photographs in an advertisement and posted the ad on a website named "List Crawler." MV2 said List Crawler is used for prostitution. Richards used his cell phone to create the ad. MV2 said her name on the ad was "Carmel Candy" and MV1's name was "Essence."

44. MV2 located and identified the ad that Richards created on List Crawler and showed it to investigators. The ad stated, "Pussy Wet & Head [fire emoji] You Bout To Love It Here One Or Two Girl Special." The ad listed a telephone number of 513-725-9361 to contact to set up an appointment. The females pictured in the ad were identified as Essence and Carmel Candy. The ad included three photos and one video of MV2. Photos in the ad depicted MV2's face, breasts, and backside. The ad also included three photos of MV1. Two of the photos depicted MV1 laying on a red, white, and dark colored striped bed comforter. One of the photos depicted MV1 nude laying supine with her legs spread fully exposing her vagina and breasts, the other photo depicted MV1 laying prone with her right hip and knee flexed wearing a black top and black underwear. The third photo depicted

[3] MV2 showed investigators her Facebook communication with Scorpio from Facebook account "Scor Pio."

MV1 from mid-thigh level to just below her neck, in a shower covered in what appeared to be soap, cupping her breasts. MV2 identified the telephone number on the ad, 513-725-9361, was the number Richards used to set up the dates.

45. In April 2023, Investigators conducted a follow up interview with MV1. MV1 was shown a BMV photo of Richards. MV1 identified the photo of Richards as the individual she knew to be Scorpio. Investigators showed MV1 a photo of the 2009 Infiniti SUV registered to Scorpio's One Stop Shop, LLC. MV1 identified the vehicle as Richards' vehicle and it was the same vehicle that Richards initially collected MV1 and MV2 when they ran away from Hope Haven on February 28. In addition, MV1 told investigators Richards drove her in the Infiniti to meet UM1 to provide UM1 oral sex in exchange for money. Investigators showed MV1 a photograph of the apartment building located at 1828 Sunset Avenue, Cincinnati, Ohio. MV1 identified the apartment building as the residence of Richards. MV1 was shown a print out of the ad from List Crawler identified by MV2 and referenced above. MV1 identified herself and MV2 in the ad. MV1 told investigators the photos were taken in Richards' apartment located at 1828 Sunset Avenue. MV1 told investigators the photos of her laying on a bed were Richards' bed in his apartment. MV1 identified the blanket in the photograph as the blanket that was on Richards' bed. MV1 told investigators that MV2 took the photo of her (MV1) in the shower at Richards' direction. Richards took the photos of MV1 laying on his bed, including the photo of MV1 laying nude in a supine position exposing her vagina and breasts. MV1 said all the photo of her were taken with Richards' iPhone.

46. Investigators identified the telephone number used on the ad as a TextMe number. Basic user information obtained from TextMe, Inc. for telephone number 513-725-9361 did

not identify Richards as the subscriber. Based upon my training and experience, I know that individuals engaged in illegal activity often utilize fictitious or misleading subscriber information to conceal their identity. However, the subscriber information identified that telephone number 513-725-9361 was utilized by an iPhone 11 Pro Max, the same phone associated with Richards' AT&T number found on the LaRosa's receipt. In addition, Richards' AT&T number had two inbound calls to the TextMe number, one on February 28, 2023 at 10:49 pm and the other on March 1, 2023 at 2:19 am. The communication activity on the TextMe number is consistent with the time frame in which Richards trafficked MV1 and MV2.

47. The last login to the TextMe account associated with telephone number 513-725-9361 was on April 6, 2023 from IP address 2603:6010:b600:918f:3008:848c:6e27:c8bc. On April 24, 2023, in response to an administrative subpoena, Charter Communications advised the above referenced IP address was assigned to the account of Kelly Richards at 1828 Sunset Avenue, apartment 26C, Cincinnati, Ohio, telephone number 513-668-6630.

48. MV2 told investigators that Richards sells fentanyl, cocaine, and marijuana. Richards gave cocaine to MV2. MV2 said Richards hid his drugs in a drawer underneath a fish tank. MV2 also saw guns at Richards' apartment.

49. MV2 told investigators that Richards took her to a hotel MV2 referred to as the "Budget" where he had arranged for males to come to the hotel and engage in sex with MV2 in exchange for money. MV2 did not remember the name of the hotel, but remembered there was another hotel right next to it. MV2 believed the hotel was close to a White Castle restaurant. MV2 said they made her lay down and did things to her and she had to give the money to Richards. MV2 also told investigators Richards would take her to houses. She

would go into the houses and they would do what they wanted to her, after which she would go back to Richards' car and he would take the money. When asked what they wanted to do to her, MV2 said they "just wanted to fuck." Richards had another person pay for the hotel rooms.

50. MV2 showed investigators text communication she had with Richards over Facebook Messenger. On March 18, 2023, Richards sent the following message to MV2, "Sup man you know hella people keep calling for you." MV2 said Richards was referencing individuals calling the number on the ad for dates. On March 20, 2023, Richards sent the following message to MV2: "I'm waiting to grab this room" and "I'm calling around now." MV2 said Richards was talking about a hotel. MV2 asked where he was at and Richards responded, "Sharonville."[4] Later in the same conversation, Richards sent the following message to MV2, "Waiting to see if somebody show up." MV2 told investigators that Richards was referring to someone from the ad. MV2 responded, "ok hit me up ok?" then Richards text, "Not long."

51. Based upon the information provided by MV1 and MV2, and my training and experience, and through conversations with other experienced investigators, it is believed Richards utilized MV1 and MV2 for the purposes of sex trafficking.

52. Based upon the evidence in this investigation, I believe Kelly Richards produced child pornography at the residence of 1828 Sunset Avenue, apartment 26, Cincinnati, Ohio and I further believe Richards, along with other persons known and currently unknown, was involved in activities which facilitated the commercial sex trafficking MV1 and MV2. Based on the foregoing, I request the Court issue the proposed search warrants.

[4] It is known to investigators that Sharonville is an area that contains hotels utilized for prostitution.

REQUEST FOR SEALING

53. I further request the Court to order all papers in support of this application, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Nathan Holbrook

NATHAN HOLBROOK
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on May 12, 2023 by reliable electronic means, specifically, FaceTime video conference.

Stephanie K. Bowman

HONORABLE STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-3

The premises to be searched is the person of Kelly Richards, further described as a black male born on October XX, 1980, with Social Security Account Number of XXX-XX-8394. Richards is approximately 5 feet and 7 inches tall, with black hair and brown eyes. Richards has a scorpion tattoo on the left side of his face. The premises to be searched also includes any clothing Richards is wearing at the time of the search, as well as any bags or containers on Richard's person or within his reach at the time of the search. Attached is a BMV photo of Richards.

ATTACHMENT B

Particular Things to be Seized

1. Computer(s), cellphone(s), tablet(s), computer hardware (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives, diskettes, and other memory storage devices), computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography, child erotica, or to prostitution or sex trafficking of a minor.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography, or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct, or to sex trafficking or prostitution.

4. In any format or medium, all child pornography or child erotica.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer, or by other means for the purpose of distributing or receiving child pornography, visual depictions, or the prostitution or sex trafficking of a minor.

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by computer, any child pornography, visual depictions, or the prostitution or sex trafficking of a minor.

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography, visual depictions, or the prostitution or sex trafficking of a minor

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography, or the existence of sites on the Internet that contain child pornography or that cater to whose with an interest in child pornography or the prostitution or sex trafficking of a minor.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members or the prostitution or sex trafficking of a minor.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.

13. Any and all cameras, film, videotapes or other photographic equipment.

14. Any and all visual depictions of minors in order to compare the images to known and identified minor victims of sexual exploitation or sex trafficking.

15. Any and all address books, mailing lists, supplier lists, mailing address labels, and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography or any visual depictions, or the prostitution or sex trafficking of a minor.

16. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages,

and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

17. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.
18. Any records, bills, or other documents associated with internet service providers and telephone services.

19. Any records or communications in which sexually explicit material is being sent or received and any records or communications relating to prostitution or sex trafficking of a minor.